Draft Technical Specifications for Core Services: Addendum to Technical Implementation Plan

Posted for Public Comment:
September 9, 2010

Preface

The following document is an addendum to Cal eConnect's Technical Implementation Plan and was created by Sujanksy & Associates, LLC under subcontract to the California eHealth Collaborative (CAeHC) in June of 2010. The Technical Implementation Plan is intended to provide the steps necessary to operationalize California's HIE Strategic and Operational Plan. The Technical Implementation Plan and the attached addendum reflect the agreed-upon framework described in the HIE Strategic and Operational Plan for creating the core services deemed essential to establish the trusted infrastructure for HIE at the state level. The plan acknowledges the fluctuating and evolving nature of industry standards and federal requirements related to sustaining statewide HIE. This addendum provides additional information on the technical specifications required for building the Entity and Service Registries described in the Technical Implementation Plan.

Please note that in the Technical Implementation Plan, the registries are referred to as the Entity Registry and Service Registry. In some instances, the service registry is referred to as a provider registry and both registries have been referred to as a provider registry or registries. The author of the addendum chose to refer to the Service Registry as the Provider Directory Service. We acknowledge that the interchangeable use of the terms may be confusing; hence this note of clarification.

Cal eConnect is posting this specification document along with the Technical Implementation Plan to provide further insight into the purpose and value of the Core Services that Cal eConnect will provide to its HIE partners across the state. The Core Services are intended to establish the trust relationship required to enable the private and secure exchange of electronic health information. The specifications and criteria for the establishment of additional services will be made available for public comment and input as they are identified and agreed upon by the stakeholder community.

Thank you for your interest and input. To submit comments, please visit www.caleconnect.org for the RFIPC submission guidance. Deadline for submissions is September 30, 2010.

Cal eConnect, Inc.
September 9, 2010

Cal eConnect, Inc.
State Infrastructure for
Health Information Exchange

Functional Requirements and Technical Specifications

Version 0.1

June 30, 2010

Prepared by

Sujansky & Associates, LLC

DRAFT

Revision History

Version	Author/Editor	Date	Comment
0.1	Walter Sujansky	6/30/2010	

Table of Contents

Tables

Figures

1. Introduction

This document describes the functional requirements and technical specifications of the Cal eConnect infrastructure for health information exchange (HIE) in California. Cal eConnect intends to contract for the development of the key components of this infrastructure. The purpose of the document is to provide sufficient technical information to inform the RFP and contracting process.

The document is divided into the following sections:

1. *Overview of State Infrastructure for HIE*
2. *Messaging Framework*: The specifications for sending and receiving secure messages.
3. *Authorization Framework*: The specifications for validating the senders of messages
4. *Entity Registry Service*: A repository of organizations certified to use the HIE Infrastructure
5. *Provider Directory Service*: A repository of provider identity and addressing information

2. Cal eConnect State Infrastructure for HIE: Overview

The Cal eConnect State Infrastructure for HIE (the "infrastructure") consists of two general parts:

1. The specifications of an asynchronous messaging framework and authorization framework that are based on the public internet and established web-services standards. These specifications are intended to define a channel for secure, trusted communications among health care entities. Entities that faithfully implement the messaging framework will be able to reliably identify and interoperate with their counterparties.
2. A small set of shared software services that facilitate the use of the messaging framework and authorization framework. These services will enable health care entities to determine the electronic identities and electronic addresses of counterparties to whom they wish to send information, as well as to verify the identities of counterparties from whom they have received information. The shared services are the *Entity Registry Service* and the *Provider Directory Service*

The envisioned role of this infrastructure in health information exchange is further described in the California HIE Operational Plan[i]. The general technical strategy and technical architecture of this infrastructure is further described in the California HIE Implementation Plan[ii]. These documents provide important definitions and contextual information needed to evaluate the functional requirements and technical specifications described in this document. The overview below covers only the most important aspects of this background information.

2.1. Messaging Framework

The messaging model supports secure and trusted communications between *Providers*. Providers must be members of registered *Entities* and must use registered *Nodes* to send and receive information. Secure messaging entails the transmission of messages between two certified nodes, with the application of Transport-Layer Security (TLS) to mutually authenticate the nodes and to encrypt the message content "on the wire." Trusted messaging entails the inclusion of electronically signed digital artifacts (*certificates* and *assertions*) within messages to verify the identities of the sending provider and the sending entity.

The following definitions are noteworthy:

- "Entities" are legal entities that assume responsibility for (1) reliably provisioning their providers when they grant them user accounts that enable health information exchange, (2) reliably authenticating their providers when the providers engage in health information exchange, and (3) maintaining directory entries for their providers that are accurate and up to date. All providers that wish to use the infrastructure for HIE must belong to an entity that assumes these responsibilities on their behalf.
- "Providers" may be individuals (such as a physician), organizational units (such as an emergency room in a hospital), or information resources (such as an immunization registry). Providers are always the ultimate senders and recipients of health information. Providers are identified by the combination of the entity to which they belong and their unique identifier within that entity. Individuals may belong to multiple entities, in which case they will have multiple identities (similarly to the way that individuals may have multiple email addresses).
- "Nodes" are servers that are addressable on the public internet. Providers' addresses must resolve to Nodes. Nodes may be operated by the legal entities to which providers belong, or they may be operated by a separate messaging intermediary, such as an HIO or commercial HIE service. A single health information transmission may traverse multiple nodes to reach its intended recipient.

2.2. Authorization Framework

The Authorization Framework is intended to provide assurance to both the sender and the recipient of health information that their counterparties are the providers they claim to be. To anchor the trust model, a trusted Certificate Authority certifies all healthcare entities authorized to initiate and receive HIE transactions. The certification process confirms that the entities legitimately exist and follow adequate practices for securing their I.T. resources and user accounts.

Certified entities are responsible for creating and managing accounts for the providers that fall under their jurisdictions. When these providers seek to exchange health information via the infrastructure, the entities are also responsible for properly authenticating them and for generating the appropriate authorization artifacts.

The principle of local autonomy. The trust model entails that providers are provisioned and authenticated by their entities at the origination point of HIE transactions, rather than by the HIE infrastructure itself. The HIE infrastructure includes no services for provider identity management or provider authentication, only the facility to communicate authentication and attribute information about providers that was generated by their entities. Similarly, the model entails that all authorization decisions regarding protected health information are made at the destination point of HIE transactions, rather than within or by the HIE infrastructure itself. The HIE infrastructure includes no services to centrally manage access control rules, patient consent, etc.. The infrastructure contains only the facility to communicate attribute and authorization information about providers who are transmitting or requesting patient-specific health information. It is the responsibility of the provider or entity at the destination point to make authorization decisions based on this information.

2.3. Shared Software Services

The *Entity Registry Service* is a searchable repository of digital certificates for certified entities. The role of this service is to provide a directory of entities that may be accessed to determine an entity's digital identity and to look up the address of the entity's Provider Directory.

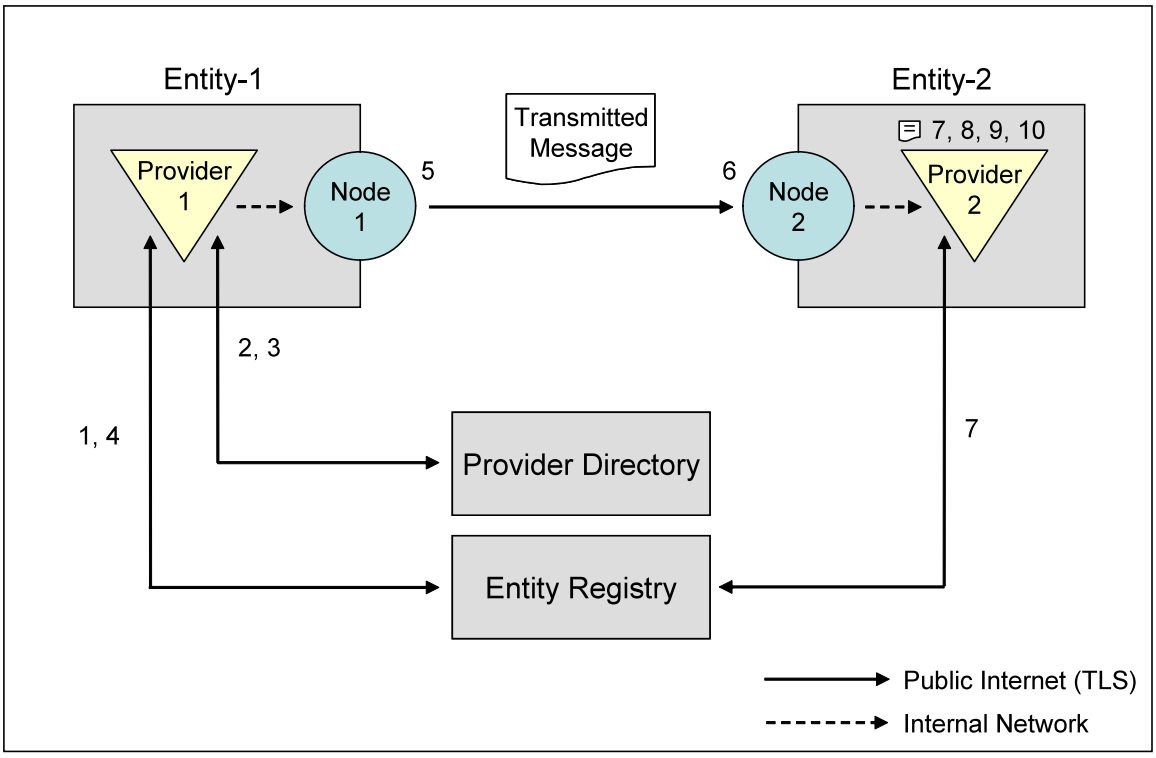
The *Provider Directory Service*[1] is a directory of providers organized by the legal entities' to which they belong. For each provider listed, the directory includes a set of message-addressing and message-formatting specifications, which may vary by the type of transaction (e.g., "Send discharge summary" versus "Send lab result" versus "Request patient summary"). These specifications inform other entities of where and how to communicate electronically with the listed providers.

A shared ("global") Provider Directory Service will be implemented as part of the Cal eConnect infrastructure. This directory will contain only a subset of all of the providers accessible via the infrastructure, however. Other organizations will also host "local" instances of the Provider Directory Service to publish the addresses of providers. These organizations may be large provider organizations, HIOs, or commercial entities that provide HIE services. In all cases, local instances of the Provider Directory Service will conform to the same web-services API as the global Provider Directory Service, to enable systems to access provider directory information in a uniform manner regardless of where it is hosted.

2.4. An Example Transaction

The infrastructure is intended to supported secure communications that are trusted by both the senders and recipients of HIE transactions. Figure 2.1 illustrates how the components of the infrastructure enable the sender and the recipient of a message to validate its destination and source (respectively). The description below this figure describes the steps involved. In this example, the sender is Provider-1, who belongs to Entity-1 and uses Node-1 for HIE transactions. The recipient is Provider-2, who belongs to Entity-2 and uses Node-2 for HIE transactions.

Figure 2.1 Use of infrastructure components for secure and trusted messaging



Sender (Provider-1):

[1] The Provider Directory Service is referred to as the Service Registry in the Technical Implementation Plan.

(1) The sender accesses the Entity Registry and retrieves the record for the entity to which the intended recipient belongs (See Section 5). This entity record includes a digital certificate from a trusted Certificate authority, certifying the entity's identity and public key. The record also includes the electronic address of the Provider Directory in which the entity's provider records are published.

(2) The sender accesses the indicated provider directory and retrieves the provider record of the intended recipient (See Section 6.2.1.1). This record enables the sender to confirm the identity of the recipient by inspecting her demographic attributes, National Provider Identifier, etc. Each provider record in this directory is digitally signed by the entity to which the provider belongs.

(3) The sender retrieves the address records of the intended recipient from the provider directory Service (See Section 6.2.1.3). These records enable the sender to discover and validate the address to which health information intended for the recipient should be transmitted. Each address record in this directory is digitally signed by the entity to which the recipient belongs.

(4) The signature of the entity is validated by checking the entity's digital certificate, which is signed by the central Certificate Authority. The certificate establishes a chain of trust between the Certificate Authority and the published identity and address of the intended recipient. This chain enables the sender to validate that the identity and address to which it is sending the health information is legitimate and was not, for example, published by a malicious third party.

(5) Upon transmission of the health information to the published address, the node at that address is validated by inspecting its digital certificate and signature as part of the TLS handshake (See Section 3.2).

Recipient (Provider-2):

(6) The receiving node validates the sending node by inspecting its digital certificate and signature as part of the TLS handshake.

(7) The receiving node inspects the digital certificate of the sending entity (included in the message) and validates it as a legitimate entity in the HIE infrastructure (i.e., by virtue of having a certificate signed by the Certificate Authority). See Section 4.1.2.

(8) The message signature is validated to have been generated by the sending entity, confirming origination at that entity (i.e., non-repudiation of source). See Section 4.1.2.

(9) The authentication and attribute assertions for the sending provider are inspected and validated. These assertions are digitally signed by the entity to which the sending provider belongs. The signatures establish a chain of trust between the Certificate Authority and the claimed identity of the sending provider. See Section 4.1.2.

(10) The authorization assertion from the sending provider is inspected and validated. This assertion is also digitally signed by the entity to which the initiating provider belongs. This signature establishes a chain of trust between the Certificate Authority and the authorization claims of the sending provider. See Section 4.1.2.

3. Messaging Framework

The Messaging Framework is not a software system. It is a set of specifications that defines the format and contents of information exchanged within the infrastructure. Senders and recipients of HIE transactions will use the messaging framework when transmitting health information or making requests

for health information. Interactions between providers and the Entity Registry Service or the Provider Directory Service will also use the messaging framework.

3.1. Functional Requirements

The messaging framework defines an asynchronous messaging protocol that meets three requirements:

1. It is based on non-proprietary industry standards
2. It can operationalize the security and trust models defined for HIE in California
3. It supports the types of HIE transaction types required to achieve meaningful use.

3.1.1. "Push" Message Pattern

Based on the Stage-1 meaningful use requirements, the first priority of the messaging framework will be to support a "push" message pattern. In this pattern, unsolicited transmissions of patient-specific health information are pushed from one provider to another, and appropriate acknowledgements are returned to indicate the action taken upon receipt of the message.

Transaction Types: The minimum set of transaction types that must be supported by the "push" message pattern includes

- Deliver Laboratory Test Result
- Send Hospital Discharge Summary
- Send Ambulatory Patient Summary
- Send Immunization Event
- Send Secure Message to a Provider
- Write Record(s) to Entity Registry Service
- Write Record(s) to Provider Directory Service

Push-Pattern Messaging Handshake: The basic handshake for transmitting an unsolicited message from Provider-1 using Node-1 to Provider-2 using Node-2 is

1. Provider-1 initiates transmission of a message from his messaging gateway (Node-1) to the messaging gateway designated for Provider-2 (Node-2)
2. Node-1 establishes a network connection to Node-2 over the public internet. This connection is secured via TLS (including mutual authentication and exchange of encryption key(s))
3. Node-1 transmits the message to Node-2 over this secure channel
4. Node-2 acknowledges receipt of the message over this secure channel (acknowledgement signifies that the message was conformant to the specifications of the messaging framework; it does not signify that the transmitted health information was received by Provider-2 or was accepted)
5. The secure channel is closed
6. Node-2 delivers the message to Provider-2 such that Provider-2 can review it and take appropriate action. If Node-2 is Provider-2's own information system, this processing may entail simply queuing the message in Provider-2's "in-box." If Node-2 is a messaging intermediary that is also part of the HIE infrastructure, this processing may entail forwarding the message to the recipient's node using the same messaging framework and push-pattern handshake. If Node-

2 is a messaging intermediary that routes messages only within Provider-2's institution, this processing may entail forwarding the message to Provider-2's information system using any secure and reliable network.

7. Provider-2 reviews and acts upon the message. Based on the action taken, Provider-2 formulates an acknowledgement message for the sending provider. The message will be sent from Provider-2's messaging gateway (Node-3) to the return address indicated for Provider-1 (Node-4). Note: Node-3 may be the same as Node-1, and Node-4 may be the same as Node-2, but this is not necessarily the case. The acknowledgement message will contain one of several acknowledgements specific to the type of information originally sent and the disposition of that information, such as:
    - Data Received and Accepted
    - Data Received and Not Accepted – Authorization Failure
    - Data Received and Not Accepted – Patient-Matching Failure
    - Data Received and Not Processed – Timeout (data was received but not acted upon within a specified time period)
    - …etc.
8. Node-3 establishes a secure network connection to Node-4 and transmits the acknowledgement message per steps 2 through 5 above.

3.1.2. "Pull" Message pattern

A query/response ("pull") message pattern will be required to retrieve information from the Entity Registry Service and Provider Directory Service. In addition, a query/response pattern for exchanging PHI may be required to enable providers to fulfill the stage-2 and stage-3 meaningful-use criteria. In this pattern, a request for patient-specific health information is transmitted from one provider to another, and the requested information and/or an appropriate acknowledgement is returned to the initiating provider.

Transaction Types: The minimum set of transaction types that must be supported by the "pull" message pattern includes

- Request Hospital Discharge Summary
- Request Ambulatory Patient Summary
- Request Immunization History
- Request Record(s) from Entity Registry Service
- Request Record(s) from Provider Directory Service

Pull-Pattern Messaging Handshake: The basic handshake for executing a query/response transaction initiated by Provider-1 using Node-1 and fulfilled by Provider-2 using Node-2 is

1. Provider-1 initiates transmission of a request message from his messaging gateway (Node-1) to the messaging gateway designated for Provider-2 (Node-2)
2. <Steps 2 – 6 are identical to steps 2-6 for the "push" message pattern.>
7. Provider-2 reviews and acts upon the request. Based on the action taken, Provider-2 formulates an acknowledgement message for the sending provider. The message will be sent from Provider-2's messaging gateway (Node-3) to the return address indicated for Provider-1 (Node-4). Note: Node-3 may be the same as Node-1, and Node-4 may be the same as Node-2, but this is not necessarily the case. The response will contain one of several acknowledgements

specific to the type of information originally requested and the disposition of the request, such as:

- Request Received and Accepted – Information Attached
- Request Received and Accepted – Information Pending (will be sent in a forthcoming message)
- Request Received and Not Accepted – Authorization Failure
- Request Received and Not Accepted – Patient-Consent Failure
- Request Received and Not Accepted – Patient-Matching Failure
- Request Received and Not Processed – Timeout (request was received but not acted upon within a specified time period)

8. Node-3 establishes a secure network connection to Node-4 and transmits the message per steps 2 through 8 of the "push" pattern above (including an acknowledgement from the original requestor that the information was received and accepted).

3.2. Technical Specifications

The messaging framework will use SOAP messages transmitted over HTTP with Transport Level Security (TLS). More specifically, the framework will conform to the WS-I Basic Profile 2.0[iii] and the WS-I Security Profile 1.1[iv]. These profiles use the web-services standards specified in Table 3.1, but prescribe further constraints to improve interoperability among conforming systems.

Table 3.1. Standards specified by WS-I Basic Profile 2.0 and WS-I Security Profile 1.1

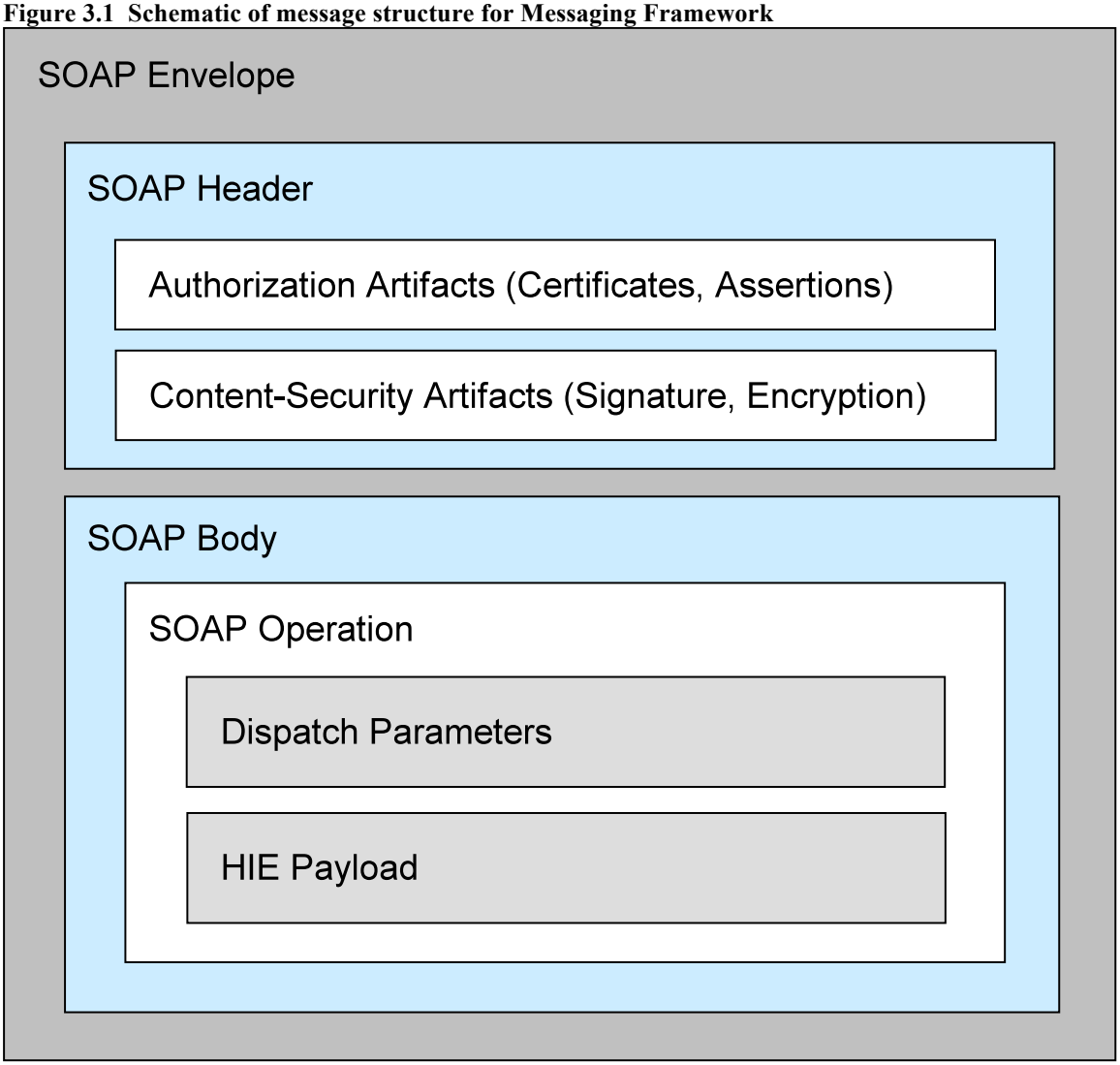
Specification	Version	Comments
SOAP	1.2	
SOAP Message Encoding Style = Document Literal		
XML Schema	1.0	
WSDL	1.1	
HTTP	1.1	
Transport Layer Security (TLS)	1.0	Equivalent to SSL v3.0
Advanced Encryption Standard (AES) with 128-bit key length		Symmetric encryption algorithm
Secure Hash Algorithm 1 (SHA-1)		Verification of message integrity in TLS
X.509 Token Profile	1.0	Digital certificates for nodes communicating via TLS

Note that these specifications are consistent with the messaging platform specifications for NHIN-Exchange[v] as well as the transport and security requirements for EHR certification per the ONC Interim Final Rule[vi].

3.2.3. General Message Structure

Figure 3.1 summarizes the general structure of SOAP messages specified by the messaging framework. The details of this structure will be prescribed by the WS-I Basic Profile 2.0 and the WS-I Security Profile 1.1, as well as additional constraints specified by the contractor.

Figure 3.1 Schematic of message structure for Messaging Framework



3.2.3.1. Authorization Artifacts

This section contains the digital certificate of the sending entity and the authentication, attribute, and authorization assertions of the sending provider. These artifacts are further described in See Section 4.

3.2.3.2. Content-Security Artifacts

This section contains the digital signature for the SOAP body, to verify that the dispatch parameters and HIE payload were not altered during the message's transit (required). The signature method is specified in Section 3.2.4. The section may also contain WS-Security headers required for the encryption of the HIE Payload (optional). The encryption method, if one is used, is specified in Section 3.2.4.

3.2.3.3. SOAP Operation

This section contains the name of the operation that the message is intended to perform and the parameters and HIE contents related to that operation. For example, SOAP Operations for the "push" message pattern may be entitled "SendDischargeSummary" and "AcknowledgeDischargeSummary".

3.2.3.4. Dispatch Parameters

These data elements provide meta-information about the intended operation, including:

1. The identifier of the intended recipient. The format for this identifier is described in Section 6.2.1.4.
2. The identifier of the transaction type being requested (e.g., "SendDischargeSummary", "RequestImmunizationHistory")
3. The identifier of the protocol being used to conduct the transaction (e.g., "ELINCS vHL7-R1")
4. The return address for responses to the transmitted message (whether acknowledgement messages or the requested patient information)

The contents of this section are never encrypted, because they may be required by messaging intermediaries and message-processing systems to correctly route and process incoming HIE messages. These contents may not, therefore, contain any protected health information.

3.2.3.5. HIE Payload

This section contains all of the protected health information communicated in the message. For "push" transactions, the HIE payload contains the transmitted patient data, including patient demographic information and identifiers. For data requests in "pull" transactions, the HIE payload contains any patient demographic information or identifiers used to specify the patient for whom data are requested. For data responses in "pull" transaction, the HIE payload contains the transmitted patient data.

Note that the HIE Payload section is the only part of the message that may contain protected health information. This section may optionally be encrypted using the receiving entity's private key or the receiving provider's private key.

3.2.4. Content Security

Message Signature: XML Signature standard (per WS-I Security Profile 1.1)

Canonicalization method: Exclusive Canonicalization (http://www.w3.org/2001/10/xml-exc-c14n#).

Signature method: RSA signing and verification (http://www.w3.org/2000/09/xmldsig#rsa-sha1)

Message Encryption: XML Encryption Standard (per WS-I Security Profile 1.1)

Encryption method: 128-bit AES (http://www.w3.org/2001/04/xmlenc#aes128-cbc)

4. Authorization Framework

The Authorization Framework is not a software system. It is a set of specifications that defines a trust model for exchanging protected health information using the messaging framework.

4.1. Functional Requirements

The authorization framework consists of two parts: (1) a *Certificate Authority* that certifies entities as participants in good standing in the HIE infrastructure, and (2) a set of *authorization artifacts* that enable sending entities to formally attest to the source of messages in a manner that receiving entities or receiving providers can validate.

4.1.1. Certificate Authority

The specific identity, responsibilities, and processes of the certificate authority (CA) are yet to be determined. In any case, the CA will need to interact with the technical infrastructure in several ways:

1. The CA will create and sign digital certificates for qualified entities and add these certificates to the Entity Registry.
2. When digital certificates expire, the CA will create new certificates and add these to the Entity Registry.
3. The CA will revoke existing certificates and add new certificates to the Entity Registry when the contents of certificates need to be updated (e.g., the legal name of the entity has changed)
4. The CA will revoke existing certificates in the Entity Registry if entities are judged to have violated the terms of participation in the state HIE infrastructure (following a formal adjudication process).
5. The CA will periodically publish the list of revoked certificates (revocation list) to all participants in the state HIE infrastructure.

The Entity Registry Service described in Section 5 will need to support these operations in a highly secure manner. The digital certificates stored in the Entity Registry will form the foundation of the authorization model for HIE.

4.1.2. Authorization Artifacts

The authorization artifacts must express in a trusted manner the following claims about the message in which they are included:

1. The identity of the sending entity. This claim is expressed through two artifacts:

   (A) A *digital certificate* whose subject is the sending entity and which is signed by the certificate authority. The digital certificate includes attributes of the sending entity sufficient to unambiguously identify it, as well as the sending entity's PKI public key.

   (B) The *digital signature* of the sending entity, such that message recipients may validate the signature using the entity's public key. The purpose of the digital signature is to authenticate the sending entity and to validate the integrity of the transmitted message. The digital signature is specifically *not* intended as any form of medical attestation of the HIE payload. Such attestation, if required, should be sent as part of the HIE payload itself.

2. The identity of the sending provider. This claim is expressed through two artifacts:

   (A) an *authentication assertion* that indicates the provider sending the message was properly authenticated, as well as the manner and time of authentication.

   (B) An *attribute assertion* that associates the provider who sent the message with a set of attributes sufficient to unambiguously identify the provider

Both of these assertions are signed by the sending entity, such that message recipients may validate the signatures using the entity's public key. By signing these assertions, the sending entity is effectively attesting to the identity and authentication of the sending provider.

3. The sending provider's stated reason for the exchange of PHI. This claim is expressed through an *authorization assertion* that contains at least two pieces of information:

   (A) The professional role of the sending provider (e.g., physician, nurse, pharmacist, administrator)

   (B) The "reason for use" of the PHI that the sending provider is transmitting or requesting (e.g., "patient treatment," "public health," "research," "payment").

   The authorization assertion is also signed by the sending entity, such that message recipients may validate the signature using the entity's public key. By signing this assertion, the sending entity is attesting that the sending provider claimed the indicated role and reason for use as justification for the exchange of PHI.

Table 4.1 represents the requirements for each of these artifacts depending on the kind of message transmitted via the messaging framework. Note that the matrix distinguishes between messages relating to PHI and messages related to information stored in the Entity Registry Service or Provider Directory Service. See Section 3.1.1 and 3.1.2 for more information about the sequence of messaging that takes place during push and pull transactions.

Table 4.1. Matrix of authorization artifacts required, by message pattern and message type

Message Pattern	Type of Data	Type of Message	Authorization Artifact ("R" = Required)				
			Digital Certificate (Entity)	Digital Signature (Entity)	Authentication Assertion (Provider)	Attribute Assertion (Provider)	Authorization Assertion (Provider)
Push	PHI	Send PHI	R	R	R	R	R
		Ack to send	R	R	R	R	
	ERS/PDS Records	Write ERS/ PDS Records	R	R	R	R	
		Ack to write	R	R	R	R	
Pull	PHI	Request PHI	R	R	R	R	R
		Ack to request	R	R	R	R	
		Deliver PHI	R	R	R	R	R
		Ack to delivery	R	R	R	R	
	ERS/PDS Records	Request ERS Records					
		Request PDS Records	R	R	R	R	
		Ack to request					
		Deliver ERS or PDS Records					

Note: "ERS" = Entity Registry Service; "PDS" = Provider Directory Service; "R" = Required.

4.2. Technical Specifications

The authorization artifacts will be represented as data structures consistent with WS-I Security Profile 1.1[iv]. The specific standards for each type of artifact are listed in Table 4.2, with details available in the documentation of the WS-I Security Profile.

Table 4.2. Standards specifications for authorization artifacts

Authorization Artifact	Specification	Version	Comments
Digital Certificate (Entity)	X.509 Token Profile	1.0	Signed by certificate authority
Digital Signature (Entity)	XML Signature	1.0	Signature of sending entity via Exclusive Canonicalization and RSA-SHA-1 encryption (See Section 3.4 in NHIN Authorization Framework v1.0[vii])
Authentication Assertion (Provider)	SAML Token Profile	1.1	Signed by sending entity per the specifications in this table
Attribute Assertion (Provider)	SAML Token Profile	1.1	Signed by sending entity per the specifications in this table
Authentication Assertion (Provider)	SAML Token Profile	1.1	Signed by sending entity per the specifications in this table

4.2.1. Contents of Authorization Artifacts

To conform to the Authorization Framework, the authorization artifacts appearing in HIE messages will need to contain the specific fields indicated in Table 4.3 and Table 4.4.

Table 4.3. Fields to be included in authorization artifacts, by artifact type

Provider Type	Field	Value Set/Comments
Digital Certificate (Entity)	(See Section 5.2.4 for contents of digital certificates)	
Digital Signature (Entity)	XML element formatted per the Digital Signature specification in Table 4.2	Digital signature of the sending entity over the entire SOAP Body contents (including the Dispatch Parameters). See Section 3.2.3 for specification of SOAP Body contents.
Authentication Assertion (Provider)	Unique ID of sending provider	See Section 6.2.1.4 for the provider identification system in HIE infrastructure
	Authentication method	See Section 3.3 in NHIN Authorization Framework v1.0vii
	Authentication time	See Section 3.3 in NHIN Authorization Framework v1.0vii
Attribute Assertion (Provider)	Unique ID of sending provider	See Section 6.2.1.4 for the provider identification scheme o HIE

		infrastructure
	Provider Type	See Table 4.4 below for Provider Types
	(For list of additional Provider Attributes – See Table 4.4)	The required Provider Attributes will vary by the type of provider
Authentication Assertion (Provider)	Unique ID of sending provider	See Section 6.2.1.4 for provider identification scheme
	Role of sending provider	SNOMED-CT
	"Purpose of use" for PHI	See "Purpose of use" vocabulary in NHIN Authorization Framework v1.0vii

Table 4.4. Provider attributes to be included in attribute assertion, by provider type.

Provider Type	Attribute	Value Set/Comments
Physician	Provider Unique ID	See Section 6.2.1.4 for identification scheme. Note that this is *not* the NPI, which is communicated in a separate field.
	First Name	Text
	Last Name	Text
	Middle Initial or Name	Text (optional)
	Professional Degree	Text ("MD", "DO", etc.)
	NPI	CMS NPI
	Specialty	Text name of specialty
	Relevant Institution	Text name of institution
	Institution Address	Text address, including street, city, etc.
	Contact Phone Number	10-digit phone number
	Contact Email Address	Text (optional)
NonPhysicianClinician	(Same attributes as Physician, except that NPI and Specialty are optional)	
Proxy (a provider that is conducting an HIE transaction on behalf of another provider)	Provider Unique ID	See Section 6.2.1.4 for identification scheme
	First Name	Text
	Last Name	Text
	Middle Initial or Name	Text (optional)
	Provider Type	Text (any of the provider types indicated in this table, except "Proxy")
	Relevant Institution	Text name of institution
	Institution Address	Text address, including street, city, etc.
	Contact Phone Number	10-digit phone number

	Contact Email Address	Text (optional)
	On-Behalf-Of-Provider	Full set of attributes (as specified in this table) for the provider whom the proxy is representing in the specific transaction
AdministrativeUser (any individual who is not a clinician)	Provider Unique ID	See Section 6.2.1.4 for identification scheme
	First Name	Text
	Last Name	Text
	Middle Initial or Name	Text (optional)
	Relevant Institution	Text name of institution
	Institution Address	Text address, including street, city, etc.
	Contact Phone Number	10-digit phone number
	Contact Email Address	Text (optional)
OrganizationalUnit (A department, unit, site, etc. of an entity that may be the recipient or sender of health information)	Provider Unique ID	See Section 6.2.1.4 for identification scheme
	Name	Text
	Description	Text
	Parent Institution	Text
	OrganizationalUnit Address	Text address, including street, city, etc.
	Organizational Unit Contact Name	Text
	OrganizationalUnit Contact Provider Unique ID	See Section 6.2.1.4 for identification scheme
	Organizational Unit Contact Phone Number	10-digit phone number
	OrganizationalUnit Contact Email Address	Text (optional)
InformationResource (e.g., an immunization registry, disease registry, public health surveillance system, etc.)	Provider Unique ID	See Section 6.2.1.4 for identification scheme
	Name	Text
	Description	Text
	Parent Institution	Text

Note: The list of Provider Types above is not necessarily complete

5. Entity Registry Service

The Entity Registry Service (ERS) is a secure repository of information about entities and nodes that participate in the HIE infrastructure. The repository provides a web services API for both the reading and writing of this information. Most of the information about entities and nodes within this service is stored in the form of digital certificates that are created, signed, and maintained by a designated certificate authority.

The sections below describe the functional, technical, and performance requirements of the service.

5.1. Functional Requirements

The ERS supports both read and write access via a web services API.

5.1.2. Read Access

Read access to the ERS is broadly available from any node that is, itself, registered in the ERS. The retrieval of information from the ERS is intended to meet the following needs of participants in the HIE infrastructure:

1. Determination of whether an organization is registered in the ERS as a certified entity approved to participate in the HIE infrastructure. This query will enable HIE participants to discover an organization's ERS record (and access the information therein) when the entity's unique ID is not known.
2. Look up of the address at which a known entity's provider directory may be accessed. This query will enable HIE participants to discover the provider directory for an entity when the entity's unique ID is already known.
3. Determine whether a node is approved to participate in the HIE infrastructure. This query will enable HIE participants to determine whether a URL address corresponds to a node that appears in the ERS.
4. Access to the list of digital certificates for entities and nodes that have been revoked by the certificate authority ("revocation list").

To meet these needs, the ERS will provide the following web-service functions:

Table 5.1. API functions for read access to Entity Registry Service

Function	Input Parameter(s)	Return Parameter(s)
Search for entity by name	Text Search Term(s)	Unique IDs, legal names and DBA names of matching entities
Retrieve entity record by unique ID	Unique ID of entity within ERS	Digital certificate of the specified entity
Retrieve address of provider directory by entity's unique ID	Unique ID of entity within ERS	Electronic address of the entity's provider directory service
Retrieve node record by unique ID	Unique ID of node within ERS	Digital certificate of the specified node
Retrieve revocation list for entities	<none>	Most recent revocation list for entities

Retrieve revocation list for nodes	<none>	Most recent revocation list for nodes

As specified in Table 4.1, no authorization artifacts are required for requesting information from the ERS. However, because such requests are made using the Messaging Framework, the requests must originate from a certified HIE node.

The data structure and contents of the digital certificates for entities and nodes are specified in Section 5.2.4.

Certificate revocation lists (CRLs) will be published at a frequency that is TBD, pending policy decisions.

5.1.3. Write Access

Write access to the ERS is tightly controlled. The updating of information in the ERS is intended to meet the following needs of the HIE infrastructure:

1. Entering, replacing, and revoking the digital certificates of entities that participate in the HIE infrastructure. These operations will be available only to the certificate authority.
2. Entering, replacing, and revoking the digital certificates of nodes that participate in the HIE infrastructure. These operations will be available only to the certificate authority.
3. Requesting the creation, replacement, or revocation of a digital certificate for a node that participates in the HIE infrastructure. These requests will be made by entities to update the nodes that they control. In certain cases and with the proper authorization, such requests may be fulfilled automatically (i.e., without human intervention). For example, if an entity needs to revoke the digital certificate of a node that has been compromised, the entity could request that this be effected immediately.

To meet these needs, the ERS will provide the following web-service functions:

Table 5.2. API functions for write access to Entity Registry Service

Function	Input Parameter(s)	Return Parameter(s)
Insert new certificate - entity	Digital certificate for entity	Acknowledgement (success/fail)
Insert new certificate - node	Digital certificate for node	Acknowledgement (success/fail)
Replace existing certificate - entity	Unique ID of Entity, Serial # of certificate to revoke, New digital certificate for entity	Acknowledgement (success/fail)
Replace existing certificate - node	Unique ID of node, Serial # of certificate to revoke, New digital certificate for node	Acknowledgement (success/fail)
Revoke existing certificate - entity	Unique ID of entity, Serial # of certificate to revoke	Acknowledgement (success/fail)
Revoke existing certificate - node	Unique ID of node, Serial # of certificate to revoke	Acknowledgement (success/fail)
Request new certificate – node (Request for a new node certificate from entity which will	Requested contents of the digital certificate – See Section 5.2.4	Acknowledgement (success/fail/review pending) Copy of created certificate if

be responsible for the node)		success
Request replacement of existing certificate – node (Request for an updated node certificate from entity which is responsible for the node)	Unique ID of node, Serial # of certificate to revoke, Requested contents of the new digital certificate – See Section 5.2.4	Acknowledgement (success/fail review pending) Copy of created certificate if success
Request revocation of existing certificate - node (Request to revoke node certificate from entity which is responsible for node)	Unique ID of node, Serial # of certificate to revoke	Acknowledgement (success/fail review pending)

The data structure and contents of the digital certificates for entities and nodes are specified in Section 5.2.4.

As specified in Table 4.1, a number of authorization artifacts are required to update information in the ERS. In addition, all such updates and requests for updates will be rigorously logged by the ERS.

5.2. Technical Requirements

5.2.4. Content Model

Each record within the ERS will contain a X.509 v3 digital certificate[viii] stored as a binary security token. The contents of certificates for entities and nodes will differ. The required and optional fields for each are listed in Table 5.3 and Table 5.4.

Table 5.3. Contents of digital certificates for registered entities

Field	Description
Certificate Serial Number	
Subject Name	Entity unique identifier; see Section 5.2.4.1 for naming scheme
Issuer Name	Distinguished name of certificate authority (same as "Subject" of CA's digital certificate)
Validity Interval	Interval will be determined by policy, TBD
Public Key	Entity's public key
Digital Signature	Signature of certificate authority
Entity's legal name	Text
Entity's alternative names (DBA names, acronyms, etc.) – up to five alternatives	Text
Type of Entity	Possible values include: - Hospital - Ambulatory Clinic - Integrated Delivery Network - Health Insurer - Health Information Org. - State Agency - Messaging Intermediary (the full value set is TBD)
Entity Tax ID	Text – must be a valid federal tax ID
Business Address – Full Address	Text
Business Address - City	Text (for searching)
Business Address - State	Text (for searching)
Business Address - ZipCode	Text (for searching)
URL of provider directory	Text – must be a valid URL per IETF RFC-1738[ix] (optional)

Table 5.4. Contents of digital certificates for registered nodes

Certificate Serial Number	
Subject Name	Node unique identifier; see Section 5.2.4.1 for naming scheme
Issuer Name	Distinguished name of certificate authority (same as "Subject" of CA's digital certificate)
Validity Interval	Interval will be determined by policy, TBD
Public Key	Entity's public key
Digital Signature	Signature of certificate authority
Responsible Entity	Unique ID of entity responsible for the node

Revocation Lists: Revoked entity and node certificates will be included in X.509 version 2 certificate revocation lists (CRLs), which will be published periodically via the ERS (the publication schedule is TBD, pending policy decisions). Published CRLs will be signed by the certificate authority.

5.2.4.1. Unique Identifiers – Entities and Nodes

Entities and nodes that are registered in the ERS will be uniquely identified using text strings formatted as Domain Names, as specified in IETF RFC-1034[x]. The identifier of an entity or node may be formatted as a root domain (such as "HospitalCorp.com") or as a sub-domain (such as

"ValleyMedCenter.HospitalCorp.com"). In either case, the root domain name of the identifier must be registered by the entity using the identifier. In the case of an entity certificate, the root domain name must be registered by the entity itself. In the case of a node certificate, the root domain name must be registered by the entity responsible for the node.

Example Entity IDs:

HIEEntity.ValleyMedCenter.HospitalCorp.com
ValleyMedCenter.HospitalCorp.com
HospitalCorp.com
Entity33890234.org

Example Node IDs:

HIEGateway.ValleyMedCenter.HospitalCorp.com
HIEGateway.ValleyMedCenter.com
Hie.Server153.HospitalCorp.com
Node39487.Entity203942.org

Note that the domain name used to identify an entity registered in the ERS need not be a reachable host name on the internet. For entity certificates, the domain name is the *unique identifier* of the entity and not necessarily its *network address*. Entities do not necessarily even have addresses within the HIE infrastructure (only *providers* have addresses, as described in Section 6.2.1.4).

In contrast, the domain name used to identify a node registered in the ERS must be a reachable host name on the internet. For node certificates, the domain name is both the *unique identifier* of the node and its *network address* (host name). This duality is required to support TLS authentication of nodes during message transmissions.

Note that a node may have a unique identifier that is completely different than the identifier of the entity that operates the node. For example the entity uniquely identified by "ValleyMedCenter.HospitalCorp.com" may operate the node uniquely identified by "HieServer348.SomeServerFarm.com".

5.2.5. API Specifications

The technical specifications of the ERS API will conform to the Messaging Framework and Authorization Framework specified in this document. The API for read operations will conform to the "Pull" message pattern, and the API for write operations will conform to the "Push" message pattern, as described in Section 3.1. The use of authorization artifacts for read and write transactions will conform to the specifications in Table 4.1

5.3. Performance Requirements

The performance requirements are based on the following assumptions regarding the volume of data in the ERS at steady state:

Entities: 10,000
Nodes: 50,000

The performance requirements are based on the following assumptions regarding the peak load of read and write operations:

Search for Entity Certificate by Name: 50/minute
Retrieve Entity or Node Certificate by ID: 500/minute
Retrieve Entity or Node Revocation List: 10/minute

Insert and Index Certificate (Entity or Node): 10/minute
Revoke Certificate (Entity or Node): 1/minute

Performance Requirements:

Response time per read operation: < 1 second
Response time per write operation: < 5 seconds

Availability for read and write operations: 99.99% 24x7x365

6. Provider Directory Service

The Provider Directory Service (PDS) is a secure directory of information about providers that participate in the HIE infrastructure. The term "Provider" is applied generally in this context and may refer to an individual person (such as a physician, other clinician, or administrative professional), an organizational unit (such as an emergency department), or an information resource (such as an immunization registry). *Note that the term does not necessarily refer to a physician or other health care provider.*

The PDS contains information that describes providers and specifies the electronic addresses and messaging protocols available for communicating with these providers. The PDS provides a web services API for both the reading and writing of this information. The information is stored in the form of security assertions that are created, signed, and maintained by the entities to which the providers belong. These assertions must conform to the formatting and content specifications described in this document.

Like the Entity Registry Service, the PDS will be provided by Cal eConnect as a central shared resource to support HIE. Unlike the Entity Registry Service, there may exist any number of alternative provider directories available as part of the HIE infrastructure. These alternative directories may be hosted directly by entities for their own providers, by HIOs for the entities that they serve, or by commercial interests as paid services for their client entities. In all cases, however, provider directories that are part of the HIE infrastructure must support the standard web services API described in this document.

The sections below describe the functional, technical, and performance requirements of the PDS.

6.1. Functional Requirements

The PDS supports both read and write access via a web services API.

6.1.1. Read Access

Read access to the PDS is available only to providers who belong to certified entities and use certified nodes (see Table 4.1). Access to the PDS is more tightly controlled than access to the ERS to prevent the "mining" of provider data. The retrieval of information from the PDS is intended to meet the following needs of participants in the HIE infrastructure:

1. Determination of the electronic identity of a provider with which an HIE participant would like to exchange information. This query will enable HIE participants to discover a provider's PDS record (and access the information therein) when the provider's unique ID is not known. The query will be able to search within the central shared PDS for a provider record, as well as within the entire network of alternative PDSs.
2. Determination of which types of HIE transactions a specific provider supports. This query will enable HIE participants to retrieve the set of supported transactions from a provider's PDS record when the provider's unique ID is already known.
3. Determination of the electronic address and messaging protocol to use for a specific type of transaction with a specific provider. This query will enable HIE participants to discover the

technical specifications for conducting an HIE transaction with a provider when the provider's unique ID is already known.

To meet these needs, the PDS will provide the following web-service functions:

Table 6.1. API functions for read access to Provider Directory Service

Function	Input Parameter(s)	Return Parameter(s)
Search for provider assertions - Local (i.e., search within PDS only)	Search Attribute(s): - Provider Type - Provider Name - Unique ID of Provider Entity - NPI (if applicable) - Relevant institution name - Relevant institution city [Provider Name or NPI are required]	Matching provider assertions (signed assertions – see Section 6.2.1.2)
Search for provider assertions - Global (i.e., search within PDS and all alternative provider directories)	Search Attribute(s): - Provider Type - Provider Name - Unique ID of Provider Entity - NPI (if applicable) - Relevant institution name - Relevant institution city [Provider Name or NPI are required]	Matching provider assertions (signed assertions)
Retrieve provider assertion - Local (i.e., search within PDS only)	Unique ID of provider (see Section 6.2.1.4)	Matching provider assertions (signed assertion)
Retrieve provider assertion - Global (i.e., search within PDS and all alternative provider directories)	Unique ID of provider	Matching provider assertions (signed assertion)
Retrieve address assertions - Local (i.e., search within PDS only)	Unique ID of provider	Matching address assertions (signed assertions – see Section 6.2.1.3)
Retrieve address assertions - Global (i.e., search within PDS and all alternative provider directories)	Unique ID of provider	Matching address assertions (signed assertions)
Retrieve address assertions - Local (i.e., search within PDS only)	Unique ID of provider, Transaction Type	Matching address assertions (signed assertions)
Retrieve address assertions - Global (i.e., search within PDS and all alternative provider directories)	Unique ID of provider, Transaction Type	Matching address assertions (signed assertions)

Note that the "global" search functions may need to execute an exhaustive search of the PDS and all alternative provider directories. This may be a very expensive operation, and clients will be encouraged

to execute searches locally if they know which provider directory contains the desired information (e.g., if they know the entity to which the provider belongs).

Note also that the "global" retrieval functions may need to access an alternative provider directory if the provider belongs to an entity whose provider records are not published in the PDS.

As specified in Table 4.1, a number of authorization artifacts are required for requesting information from the PDS.

The data structure and contents of provider assertions and address assertions are specified in Section 6.2.1.

6.1.2. Write Access

Write access to the PDS is also tightly controlled and confined to authenticated providers at registered entities. Provider and address Records entered into the PDS must be in the form of signed security assertions (see Section 6.2.1). These assertions must be signed by the same entity to which the subject provider belongs, as this is the mechanism by which the published addresses of providers are validated.

The writing of information to the PDS is intended to meet the following needs of the HIE infrastructure:

1. Creating, editing, and deleting provider records for those providers that an entity wishes to "publicize" in the HIE infrastructure. These operations enable entities to make the electronic identity and contact information of their providers widely available to other participants in the HIE infrastructure.
2. Creating, editing, and deleting address records for those providers that an entity wishes to "publicize" in the HIE infrastructure. These operations enable entities to publish up-to-date technical specifications regarding the address at which and messaging protocols through which their providers may be reached for purposes of HIE transactions.

To meet these needs, the ERS will provide the following web-service functions:

Table 6.2. API functions for write access to Provider Directory Service

Function	Input Parameter(s)	Return Parameter(s)
Insert new provider assertion	Provider assertion (See section 6.2.1.2)	Acknowledgement (success/fail)
Update existing provider assertion	Unique ID of existing provider assertion, Updated provider assertion	Acknowledgement (success/fail)
Delete existing provider assertion (and all child address assertions)	Unique ID of existing provider assertion	Acknowledgement (success/fail)
Insert new address assertion	Address assertion (See section 6.2.1.3)	Acknowledgement (success/fail)
Update existing address assertion	Unique ID of existing address assertion, Updated address assertion	Acknowledgement (success/fail)
Delete existing provider assertion	Unique ID of existing address assertion	Acknowledgement (success/fail)
Insert new entity record*	PDS entity record (See Section 6.2.1.1)	Acknowledgement (success/fail)
Update existing entity record*	Unique ID of existing PDS	Acknowledgement (success/fail)

	entity record, Updated PDS entity record	
Delete entity record* (and all child provider assertions)	Unique ID of existing PDS entity record	Acknowledgement (success/fail)

*These operations are available only to the administrator of the PDS to initialize an entity's use of the PDS. The creation of an entity record, for example, then allows the entity to enter its own provider and address records.

The data structure and contents of the digital certificates for entities and nodes are specified in Section 5.2.4.

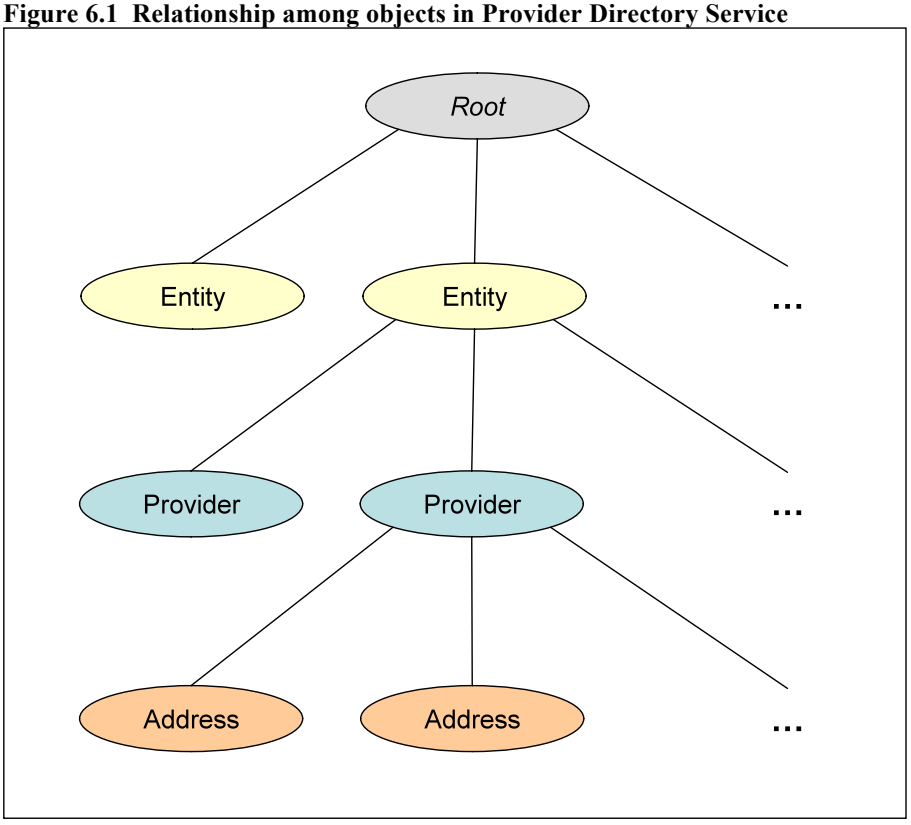
As specified in Table 4.1, a number of authorization artifacts are required to update information in the ERS. In addition, all such updates and requests for updates will be rigorously logged by the ERS.

6.2. Technical Requirements

6.2.1. Content Model

The PDS content model may be conceptualized as a hierarchy containing entities, providers, and addresses (although it is not necessarily implemented this way). Figure 6.1 illustrates the relationships among these objects.

Figure 6.1 Relationship among objects in Provider Directory Service



Providers and address records stored in the PDS (as well as in alternative provider directories) must be signed security assertions. The assertions are formatted as SAML v2.0 tokens per the SAML Token Profile v1.1. All provider and address assertions in the PDS (as well as in alternative provider directories) must be signed by the entity to which the provider belongs and under which the assertions appear in the logical hierarchy (see Figure 6.1).

The contents of provider assertions and address assertions are different, as specified in Sections 6.2.1.2 and 6.2.1.3.

6.2.1.1. Entity Record

Entity records in the Provider Directory Service will contain nothing more than the Entity Unique ID of the subject entity, and the create date of the record, and the unique ID of the record. This minimal representation will obviate the need keep this record consistent with the information in the entity's digital certificate as this information changes.

6.2.1.2. Provider Assertions

Each provider assertion will contain the fields specified in Table 6.3. Note that the specific fields within a provider assertion will vary by the provider type The types of providers that may be represented in provider assertions are the following subset of the provider types listed in Table 4.4:

- Physician
- NonPhysicianClinician
- AdministrativeUser
- OrganizationalUnit
- InformationResource

Table 6.3. Fields to be included in provider assertions

Fields	Value Set/Comments
Assertion Unique ID	A globally unique identifier for the assertion, generated by the entity at the time the assertion is created and signed
Local component of Provider Unique ID	See Section 6.2.1.4
Entity component of Provider Unique ID	See Section 6.2.1.4
Date created	
Digital Signature	Signature of signing entity. Must validate using the public key of the entity to which the provider belongs, per the entity component of the Provider Unique ID
Digital Certificate of the provider (optional)	The certificate authority for this certificate is not specified
<Remaining attributes depend on the provider type>	See Table 4.4 in Section 4.2.1 for details.

6.2.1.3. Address Assertions

Each address assertion will contain the fields specified in Table 6.4.

Table 6.4. Fields to be included in address assertions

Fields	Value Set/Comments
Assertion Unique ID	A globally unique identifier for the assertion, generated by the entity at the time the assertion is created and signed
Local component of Provider Unique ID	See Section 6.2.1.4
Entity component of Provider Unique ID	See Section 6.2.1.4
Transaction Type	The identifier of the transaction type that the address and protocol information in this assertion pertains; the value set will initially include the transactions listed in Sections 3.1.1 and 3.1.2
Date created	
Digital Signature	Signature of signing entity. Must validate using the public key of the entity to which the provider belongs, per the entity component of the Provider Unique ID
Address for the transaction	URL at which a messages for the Transaction Type indicated in this assertion can be processed on behalf of the provider indicated in this assertion. The domain name within this URL must be the identifier of a node registered in the Entity Registry Service.
Protocol for conducting the transaction	The identifier of a message-exchange protocol that (1) is specific to the type of transaction indicated in this assertion, and (2) is supported at the address indicated in this assertion. Designated protocols will include information about the sequence of message exchanges and the contents and formatting of the messages within these exchanges. The set of such protocols and the specific way they will be described is TBD.

6.2.1.4. Unique Identifiers – Providers

Providers participating in the HIE infrastructure will be uniquely identified by the combination of an *Entity Unique ID* and *Entity-Specific Provider ID*.

Entity Unique ID: The unique ID of the entity to which the provider belongs, as specified in Section 5.2.4.1. An individual (e.g., physician) may belong to multiple entities, in which case she will have multiple unique IDs for purposes of the HIE infrastructure. In this case, the Entity Unique ID component of these Provider IDs will be different (similar to the way that individuals may have multiple email addresses.

Entity-Specific Provider ID: A text string conforming to the "local-part" requirements for addresses in the internet message format specification (IETF RFC-5322[xi]). The sole exception to this specification is that the "*" character may not appear within the Entity-Specific Provider ID. This identifier must uniquely identify the provider within the context of the assigning entity. Note that the Entity-Specific Provider ID component of a Provider Unique ID need not uniquely identify providers *across* entities. In particular, two identical Entity-Specific Provider IDs associated with different entities do not necessarily refer to the same individual, organizational unit, or information resource. Similarly, an individual that belongs to two entities will not necessarily have the same Entity-Specific Provider ID within both contexts.

Delimiter: When a Provider Unique ID is represented as a single text string (e.g., in authorization assertions), the delimiter "**" is placed between the Entity-Specific Provider ID component (which appears first) and the Entity Unique ID component (which appears second).

Examples of Provider Unique IDs:

hansen.m.robert**HIEEntity.ValleyMedCenter.HospitalCorp.com
drbob**CommunityClinic.org
IZ_registry_socal**dph.chhs.gov
23857469**HospitalCorp.com

Note: The "@" character is not used as the delimiter in Provider Unique IDs to (1) avoid confusion with email addresses and (2) allow Provider Unique IDs to be used as the local-parts of email addresses.

6.2.2. API Specifications

The technical specifications of the PDS API will conform to the Messaging Framework and Authorization Framework specified in this document. The API for read operations will conform to the "Pull" message pattern, and the API for write operations will conform to the "Push" message pattern, as described in Section 3.1. The use of authorization artifacts for read and write transactions will conform to the specifications in Table 4.1.

6.3. Performance Requirements

The performance requirements are based on the following assumptions regarding the volume of data in the PDS at steady state (note that the information for approximately 2/3rds of providers is expected to be stored in alternative provider directories rather than the PDS):

Entities: 5,000
Providers: 25,000
Addresses: 150,000

The performance requirements are based on the following assumptions regarding the peak load of operations against the PDS:

Search for provider assertions by attributes: 50/minute
Retrieve provider assertion by Provider ID: 500/minute
Retrieve address assertion by Provider ID: 100/minute

Insert and index provider assertion: 10/minute
Insert address assertion: 1/minute

Performance Requirements:

Response time – local provider search operation: < 3 second
Response time – global provider search operation: < 30 second
Response time – provider retrieval operation: < 1 second
Response time – address retrieval operation: < 1 second
Response time per write operation: < 5 seconds

Availability for read and write operations: 99.99% 24x7x365

7. Test Harness

As part of the development of the HIE infrastructure, an application will be needed to serve as a test harness for the Entity Registry Service, Provider Directory Service, Messaging Framework, and Authorization Framework. This application should have the following features:

- Program logic, user interface, and API for submitting web-services calls to the ERS and PDS via the Messaging and Authorization Frameworks. This module should enable a user to view and validate the entity, provider, and address information retrieved from these services and to use this information to formulate HIE transactions (e.g., the sending or requesting of a hospital discharge summary). The module should also enable a user to create entity certificates and provider/address assertions and to enter these into the Entity Registry Service and Provider Directory Service, respectively.
- Program logic, user interface, and API for conducting HIE transactions using the Messaging Framework and Authorization Framework. This module should enable a user to send or receive PHI in the form of a document transmitted as the "HIE Payload" of a message transmission. The module should also generate the appropriate authorization artifacts to conduct these transactions, as well as verify authorization artifacts sent by counterparties.
- For demonstration purposes, the application should be available as a web-based portal that can be accessed remotely. The application should have a small number of sample document available (such as lab results, discharge summaries, ambulatory patient summaries, and immunization events), as well as a viewer for these document types.

[i] See http://www.ehealth.ca.gov/eHealthPlan/tabid/72/Default.aspx Section 5, pp. O-53 – O-80. Note that the "Provider Identity Service" as defined in this document is not included as a component of the infrastructure for its initial implementation.

[ii] See http://www.caleconnect.org/?page_id=23 Appendix 3 and Appendix 4. Note that the following components of the infrastructure defined in this document are not included as a component of the infrastructure for its initial implementation: Patient Discovery, Lab Results Clearinghouse, Publish/Subscribe message pattern.

[iii] See http://www.ws-i.org/Profiles/BasicProfile-2_0(WGD).html for detailed technical specifications.

[iv] See http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html for detailed technical specifications.

[v] See http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_910523_0_0_18/NHIN_MessagingPlatformProductionSpecification_v2.0.pdf for detailed specifications of the NHIN Messaging Platform.

[vi] See http://edocket.access.gpo.gov/2010/pdf/E9-31216.pdf

[vii] See http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_910545_0_0_18/NHIN_AuthorizationFrameworkProductionSpecification_v2.0.pdf

[viii] See http://www.ietf.org/rfc/rfc3280.txt

[ix] See http://www.ietf.org/rfc/rfc1738.txt

[x] See http://www.ietf.org/rfc/rfc1034.txt

[xi] See http://www.ietf.org/rfc/rfc5322.txt